



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,005	10/30/2003	Michael Scheidell	1012-003U	1429
29973 7590 11/21/2007 CAREY, RODRIGUEZ, GREENBERG & PAUL LLP ATTN: STEVEN M. GREENBERG, ESQ. 950 PENINSULA CORPORATE CIRCLE SUITE 3020 BOCA RATON, FL 33487			EXAMINER SHERKAT, AREZOO	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 11/21/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/699,005

Applicant(s)

SCHEIDELL, MICHAEL

Examiner

Arezoo Sherkat

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 October 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 9-11 and 14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 9-11 and 14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Response to Amendment

This office action is responsive to Applicant's amendment received on 9/7/2007. Claims 1-8, 12-13, and 15-20 are cancelled. Claims 9 and 14 are amended. Claims 9-11 and 14 are pending.

Allowable Subject Matter

The indicated allowability of claims 9-11 and 14 is withdrawn in view of the newly discovered reference(s) to Hrabik et al. (U.S. Publication No. 2002/0178383 and Hrabik hereinafter). Rejections based on the newly cited reference(s) follow.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 9-11 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Hrabik et al. (U.S. Publication No. 2002/0178383 and Hrabik hereinafter).

Regarding claim 9, Hrabik discloses a computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;

an edge database log coupled to the different log analyzers logging attacks upon the different external networks, an intrusion detector coupled to a client network and configured to detect external attacks upon the client network (i.e., security subsystem 50 on ActiveGuard 52 – fig. 2)(par. 39-48), an analyzer coupled to said intrusion detector (i.e., Log Analyzer 504) for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log (par. 55-57), and

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., counteraction mechanism 510 to address the events)(par. 61), a second intrusion detector for detecting external attacks upon a second computer network (i.e., security master system 60), and a second analyzer (i.e., Enterprise Event Analyzer 508/global event analyzer) coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof (par. 59-60), wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison (par. 61).

Regarding claim 10, Hrabik discloses the system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks (par. 59-60).

Regarding claim 11, Hrabik discloses the system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks (par. 65-68).

Regarding claim 14, Hrabik discloses a method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network, detecting an attack on a client network (par. 55-57), classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network (par. 59), prioritizing handling of the detected attack if the attack is classified as a general attack (par. 60), and generating a second alert in response to the presence of the match, wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network (i.e., alerting both master security systems 50 and 60)(par. 61).

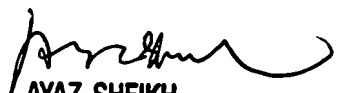
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Art Unit 2131
Nov. 16, 2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100